

Schematic Cut elimination and the Ordered Pigeonhole Principle

[Extended Version]

David Cerna¹ and Alexander Leitsch²

¹ Research Institute for Symbolic Computation (RISC)
Johannes Kepler University, Linz, Austria
dcerna@risc.uni-linz.ac.at

² Logic and Theory Group
Technical University of Vienna
leitsch@logic.at

Abstract. In previous work, an attempt was made to apply the *schematic CERES method* [8] to a formal proof with an arbitrary number of Π_2 cuts (a recursive proof encapsulating the infinitary pigeonhole principle) [5]. However the derived schematic refutation for the *characteristic clause set* of the proof could not be expressed in the formal language provided in [8]. Without this formalization a *Herbrand system* cannot be algorithmically extracted. In this work, we provide a restriction of the proof found in [5], the *ECA-schema* (*Eventually Constant Assertion*), or *ordered infinitary pigeonhole principle*, whose analysis can be completely carried out in the framework of [8], this is the first time the framework is used for proof analysis. From the refutation of the clause set and a substitution schema we construct a *Herbrand system*.

1 Introduction

For his famous *Hauptsatz* [9], Gerhard Gentzen developed the sequent calculus **LK**. Gentzen went on to show that the *cut* inference rule is redundant and in doing so, was able to show several results on consistency and decidability. The method he developed for eliminating cuts from **LK**-derivations works by inductively reducing the cuts in a given **LK**-derivation to cuts which either have a reduced *formula complexity* and/or reduced *rank* [12]. This method of cut elimination is known as *reductive cut elimination*. A useful consequence of cut elimination for the **LK**-calculus is that cut-free **LK**-derivations have the *subformula property*, i.e. every formula occurring in the derivation is a subformula of some formula in the end sequent. This property admits the construction of *Herbrand sequents* and other objects which are essential in proof analysis.

By using the technique of cut-elimination, it is also possible to gain mathematical knowledge concerning the connection between different proofs of the same theorem. For example, Jean-Yves Girard's application of cut elimination to the Fürstenberg-Weiss' proof of van der Waerden's theorem [10] resulted in

the *analytic* proof of van der Waerden’s theorem as found by van der Waerden himself. From the work of Girard, it is apparent that interesting results can be derived from eliminating cuts in “mathematical” proofs.

A more recently developed method of cut elimination, the CERES method [3], provides the theoretic framework to directly study the cut structure of **LK**-derivations, and in the process reduces the computational complexity of deriving a cut-free proof. The cut structure is transformed into a clause set allowing for a clausal analysis of the resulting clause form. Methods of reducing clause set complexity, such as *subsumption* and *tautology elimination* can be applied to the characteristic clause set to increase the efficiency. It was shown by Baaz & Leitsch in “Methods of cut Elimination” [4] that this method of cut elimination has a *non-elementary speed up* over reductive cut elimination.

In the same spirit of Girard’s work, the CERES method was applied to a formalization of Fürstenberg’s proof of the infinitude of primes [1]. Instead of formalizing the proof as a single proof (in second-order arithmetic) it was represented as a sequence of first-order proofs enumerated by a single numeric parameter indexing the number of primes assumed to exist (leading to a contradiction). The resulting schema of clause sets was refuted for the first few instances by the system CERES. The general refutation schema, resulting in Euclid’s construction of primes, was specified on the mathematical meta-level. At that time no object-level construction of the resolution refutation schema existed.

A straightforward mathematical formalization of Fürstenberg’s proof requires induction. In higher-order logic, induction is easily formalized via the comprehension principle. However in first-order, an induction rule or induction axioms have to be added to the **LK**-calculus. As it was shown in [8], ordinary reductive cut elimination does not work in the presence of an induction rule in the **LK**-calculus. There are, however, other systems [11] which provide cut-elimination in the presence of an induction rule; but these systems do not produce proofs with the subformula property, which is necessary for Herbrand system extraction.

In “Cut-Elimination and Proof Schemata” [8], a version of the **LK**-calculus was introduced (**LKS**-calculus) allowing for the formalization of sequences of proofs as a single object level construction, i.e. *proof schema*, as well as a framework for performing a CERES-type cut elimination on proof schemata. Cut elimination performed within the framework of [8] results in cut-free proof schemata with the subformula property.

In previous work, we applied the schematic CERES method of [8] to a proof formalized in the **LKS**-calculus[5,6]. We referred to this formal proof as the *Non-injectivity Assertion* (NiA) schema. A well known variation of the NiA-schema, of which has been heavily studied in literature, is the *infinitary Pigeonhole Principle* (PHP). Though a resolution refutation schema was found and mathematically specified [5], it was not possible to express this refutation schema within the language of [8]. The main problem was the specification of a unification and refutation schema. This issue points to a fundamental property of CERES-based schematic cut-elimination, namely that the language for specifying the refutation schema is more complex than that specifying the proof schema.

In this work we construct a formal proof for a weaker variant of the NiA-schema which we call the *Eventually Constant Assertion schema* (ECA-schema). The ECA is an encapsulation of the infinitary pigeonhole principle where the holes are ordered. For the ECA-schema a specification of the resolution refutation schema within the formalism of [8] turned out successful. In particular, we are able to extract a Herbrand system and complete the proof analysis of the ECA-schema.

The paper is structured as follows: In Sec. 2, we introduce the **LKS**-calculus and the essential concepts from [8] concerning the schematic clause set analysis. In Sec. 3, we mathematically prove the ECA-schema. We leave the formal proof, written in the **LKS**-calculus, to Appendix A. In Sec. 4, we extract the characteristic clause set from the ECA-schema and perform *normalization* and tautology elimination. In Sec. 5, we provide a refutation of the extracted characteristic clause set. In Sec. 6, we extract a Herbrand system for the refutation of Sec. 5. In Sec. 7, we conclude the paper and discuss our conjecture.

2 The LKS-calculus and Clause set Schema

In this section we introduce the **LKS**-calculus, which will be used to formalize the ECA-schema, and the schematic CERES method.

2.1 Schematic language, proofs, and the LKS-calculus

The **LKS**-calculus is based on the **LK**-calculus constructed by Gentzen [9]. When one grounds the *parameter* indexing an **LKS**-derivation, the result is an **LK**-derivation [8]. The term language used is extended to accommodate the schematic constructs of **LKS**-derivations. We work in a two-sorted setting containing a *schematic sort* ω and an *individual sort* ι . The schematic sort contains numerals constructed from the constant $0 : \omega$, a monadic function $s(\cdot) : \omega \rightarrow \omega$ as well as ω -variables \mathcal{N}_v , of which one variable, the *free parameter*, will be used to index **LKS**-derivations. When it is not clear from context, we will represent numerals as \overline{m} . The free parameter will be represented by n unless otherwise noted.

The individual sort is constructed in a similar fashion to the standard first order language [12] with the addition of schematic functions. Thus, ι contains countably many constant symbols, countably many *constant function symbols*, and *defined function symbols*. The constant function symbols are part of the standard first order language and the defined function symbols are used for schematic terms. Though, defined function symbols can also unroll to numerals and thus can be of type $\omega^n \rightarrow \omega$. The ι sort also has *free* and *bound* variables and an additional concept, *extra variables* [8]. These are variables introduced during the unrolling of defined function (*predicate*) symbols. We do not use extra variables in the formalization of the ECA-schema. Also important are the *schematic variable symbols* which are variables of type $\omega \rightarrow \iota$. Essentially second order variables, though, when evaluated with a *ground term* from the ω sort

we treat them as first order variables. Our terms are built inductively using constants and variables as a base.

Formulae are constructed inductively using countably many *predicate constants*, logical operators $\vee, \wedge, \rightarrow, \neg, \forall$, and \exists , as well as *defined predicate symbols* which are used to construct schematic formulae. In this work *iterated* \vee is the only defined predicate symbol used. Its formal specification is:

$$\varepsilon_{\vee} = \bigvee_{i=0}^{s(y)} P(i) \equiv \begin{cases} \bigvee_{i=0}^{s(y)} P(i) \Rightarrow \bigvee_{i=0}^y P(i) \vee P(s(y)) \\ \bigvee_{i=0}^0 P(i) \Rightarrow P(0) \end{cases} \quad (1)$$

From the above described term and formulae language we can provide the inference rules of the **LKE**-calculus, essentially the **LK**-calculus [12] plus an equational theory ε (in our case ε_{\vee} Eq. 1). This theory, concerning our particular usage, is a primitive recursive term algebra describing the structure of the defined function (predicate) symbols. The **LKE**-calculus is the base calculus for the **LKS**-calculus which also includes *proof links*.

Definition 1 (ε -inference rule).

$$\frac{S[t]}{S[t']} (\varepsilon)$$

In the ε inference rule, the term t in the sequent S is replaced by a term t' such that, given the equational theory ε , $\varepsilon \models t = t'$.

To extend the **LKE**-calculus with proof links we need a countably infinite set of *proof symbols* denoted by $\varphi, \psi, \varphi_i, \psi_j \dots$. Let $S(\bar{x})$ be a sequent with a vector of schematic variables \bar{x} , by $S(\bar{t})$ we denote the sequent $S(\bar{x})$ where each of the variables in \bar{x} is replaced by the terms in the vector \bar{t} respectively, assuming that they have the appropriate type. Let φ be a proof symbol and $S(\bar{x})$ a sequent, then the expression $\frac{(\varphi(\bar{t}))}{S(\bar{t})}$ is called a *proof link*. For a variable $n : \omega$, proof links such that the only ω -variable is n are called *n-proof links*.

Definition 2 (**LKE-calculus** [8]). The sequent calculus **LKS** consists of the rules of **LKE**, where proof links may appear at the leaves of a proof.

Definition 3 (**Proof schemata** [8]). Let ψ be a proof symbol and $S(n, \bar{x})$ be a sequent such that $n : \omega$. Then a proof schema pair for ψ is a pair of **LKS**-proofs $(\pi, \nu(k))$ with end-sequents $S(0, \bar{x})$ and $S(k+1, \bar{x})$ respectively such that π may not contain proof links and $\nu(k)$ may contain only proof links of the form $\frac{(\psi(k, \bar{a}))}{S(k, \bar{a})}$ and we say that it is a proof link to ψ . We call $S(n, \bar{x})$ the end sequent of ψ and assume an identification between the formula occurrences in the end sequents of π and $\nu(k)$ so that we can speak of occurrences in the end sequent

of ψ . Finally a proof schema Ψ is a tuple of proof schema pairs for $\psi_1, \dots, \psi_\alpha$ written as $\langle \psi_1, \dots, \psi_\alpha \rangle$, such that the **LKS**-proofs for ψ_β may also contain n -proof links to ψ_γ for $1 \leq \beta < \gamma \leq \alpha$. We also say that the end sequent of ψ_1 is the end sequent of Ψ .

We will not delve further into the structure of proof schemata and instead refer the reader to [8]. We now introduce the *characteristic clause set schema*.

2.2 Characteristic Clause set Schema

The construction of the characteristic clause set as described for the CERES method [3] required inductively following the formula occurrences of cut formula ancestors up the proof tree to the leaves. However, in the case of proof schemata, the concept of ancestors and formula occurrence is more complex. A formula occurrence might be an ancestor of a cut formula in one recursive call and in another it might not. Additional machinery is necessary to extract the characteristic clause term from proof schemata. A set Ω of formula occurrences from the end-sequent of an **LKS**-proof π is called a *configuration* for π . A configuration Ω for π is called relevant w.r.t. a proof schema Ψ if π is a proof in Ψ and there is a $\gamma \in \mathbb{N}$ such that π induces a subproof $\pi \downarrow \gamma$ of $\Psi \downarrow \gamma$ such that the occurrences in Ω correspond to cut-ancestors below $\pi \downarrow \gamma$ [7]. Note that the set of relevant cut-configurations can be computed given a proof schema Ψ . To represent a proof symbol φ and configuration Ω pairing in a clause set we assign them a *clause set symbol* $cl^{\varphi, \Omega}(a, \bar{x})$, where a is a term of the ω sort.

Definition 4 (Characteristic clause term [8]). Let π be an **LKS**-proof and Ω a configuration. In the following, by Γ_Ω , Δ_Ω and Γ_C , Δ_C we will denote multisets of formulas of Ω - and cut-ancestors respectively. Let r be an inference in π . We define the clause-set term $\Theta_r^{\pi, \Omega}$ inductively:

- if r is an axiom of the form $\Gamma_\Omega, \Gamma_C, \Gamma \vdash \Delta_\Omega, \Delta_C, \Delta$, then $\Theta_r^{\pi, \Omega} = \{\Gamma_\Omega, \Gamma_C \vdash \Delta_\Omega, \Delta_C\}$
- if r is a proof link of the form
$$\frac{\psi(a, \bar{u})}{\Gamma_\Omega, \Gamma_C, \Gamma \vdash \Delta_\Omega, \Delta_C, \Delta}$$
 then define Ω' as the set of formula occurrences from $\Gamma_\Omega, \Gamma_C \vdash \Delta_\Omega, \Delta_C$ and $\Theta_r^{\pi, \Omega} = cl^{\psi, \Omega}(a, \bar{u})$
- if r is a unary rule with immediate predecessor r' , then $\Theta_r^{\pi, \Omega} = \Theta_{r'}^{\pi, \Omega}$
- if r is a binary rule with immediate predecessors r_1, r_2 , then
 - if the auxiliary formulas of r are Ω - or cut-ancestors, then $\Theta_r^{\pi, \Omega} = \Theta_{r_1}^{\pi, \Omega} \oplus \Theta_{r_2}^{\pi, \Omega}$
 - otherwise, $\Theta_r^{\pi, \Omega} = \Theta_{r_1}^{\pi, \Omega} \otimes \Theta_{r_2}^{\pi, \Omega}$

Finally, define $\Theta^{\pi, \Omega} = \Theta_{r_0}^{\pi, \Omega}$ where r_0 is the last inference in π and $\Theta^\pi = \Theta^{\pi, \emptyset}$. We call Θ^π the characteristic term of π .

Clause terms evaluate to sets of clauses by $|\Theta| = \Theta$ for clause sets Θ , $|\Theta_1 \oplus \Theta_2| = |\Theta_1| \cup |\Theta_2|$, $|\Theta_1 \otimes \Theta_2| = \{C \circ D \mid C \in |\Theta_1|, D \in |\Theta_2|\}$.

The characteristic clause term is extracted for each proof symbol in a given proof schema Ψ , and together they make the *characteristic clause set schema* for Ψ , $CL(\Psi)$.

Definition 5 (Characteristic Term Schema[8]). Let $\Psi = \langle \psi_1, \dots, \psi_\alpha \rangle$ be a proof schema. We define the rewrite rules for clause-set symbols for all proof symbols ψ_β and configurations Ω as $cl^{\psi_\beta, \Omega}(0, \bar{u}) \rightarrow \Theta^{\pi_\beta, \Omega}$ and $cl^{\psi_\beta, \Omega}(k+1, \bar{u}) \rightarrow \Theta^{\nu_\beta, \Omega}$ where $1 \leq \beta \leq \alpha$. Next, let $\gamma \in \mathbb{N}$ and $cl^{\psi_\beta, \Omega} \downarrow_\gamma$ be the normal form of $cl^{\psi_\beta, \Omega}(\gamma, \bar{u})$ under the rewrite system just given extended by rewrite rules for defined function and predicate symbols. Then define $\Theta^{\psi_\beta, \Omega} = cl^{\psi_\beta, \Omega}$ and $\Theta^{\Psi, \Omega} = cl^{\psi_1, \Omega}$ and finally the characteristic term schema $\Theta^\Psi = \Theta^{\Psi, \emptyset}$.

2.3 Resolution Proof Schemata

From the characteristic clause set we can construct *clause schemata* which are an essential part of the definition of *resolution terms* and *resolution proof schema* [8]. Clause schemata serve as the base for the resolution terms used to construct a resolution proof schema. One additional notion needed for defining resolution proof schema is that of *clause variables*. The idea behind clause variables is that parts of the clauses at the leaves can be passed down a refutation to be used later on. The definition of resolution proof schemata uses clause variables as a way to handle this passage of clauses. Substitutions on clause variables are defined in the usual way.

Definition 6 (Clause Schema [8]). Let b be an numeric term, \bar{u} a vector of schematic variables and \bar{X} a vector of clause variables. Then $c(b, \bar{u}, \bar{X})$ is a clause schema w.r.t. the rewrite system R :

$$c(0, \bar{u}, \bar{X}) \rightarrow C \circ X \text{ and } c(k+1, \bar{u}, \bar{X}) \rightarrow c(k, \bar{u}, \bar{X}) \circ D$$

where C is a clause with $V(C) \subseteq \{\bar{u}\}$ and D is a clause with $V(D) \subseteq \{k, \bar{u}\}$. Clauses and clause variables are clause schemata w.r.t. the empty rewrite system.

Definition 7 (Resolution Term [8]). Clause schemata are resolution terms; if ρ_1 and ρ_2 are resolution terms, then $r(\rho_1; \rho_2; P)$ is a resolution term, where P is an atom formula schema.

The idea behind the resolution terms is that in the term $r(\rho_1; \rho_2; P)$, P is the resolved atom of the resolvents ρ_1, ρ_2 . The notion of most general unifier has not yet been introduced being that we introduce the concept as a separate schema from the resolution proof schema.

Definition 8 (Resolution Proof Schema [8]). A resolution proof schema $\mathcal{R}(n)$ is a structure $(\varrho_1, \dots, \varrho_\alpha)$ together with a set of rewrite rules $\mathcal{R} = \mathcal{R}_1 \cup \dots \cup \mathcal{R}_\alpha$, where the \mathcal{R}_i (for $1 \leq i \leq \alpha$) are pairs of rewrite rules

$$\begin{aligned} \varrho_i(0, \bar{w}, \bar{u}, \bar{X}) &\rightarrow \eta_i \\ \text{and} \\ \varrho_i(k+1, \bar{w}, \bar{u}, \bar{X}) &\rightarrow \eta'_i \end{aligned}$$

where, \bar{w}, \bar{u} , and \bar{X} are vectors of ω , schematic, and clause variables respectively, η_i is a resolution term over terms of the form $\varrho_j(a_j, \bar{m}, \bar{t}, \bar{C})$ for $i < j \leq \alpha$, and η'_i is a resolution term over terms of the form $\varrho_j(a_j, \bar{m}, \bar{t}, \bar{C})$ and $\varrho_i(k, \bar{m}, \bar{t}, \bar{C})$ for $i < j \leq \alpha$; by a_j , we denote a term of the ω sort.

The idea behind the definition of resolution proof schema is that the definition simulates a recursive construction of a resolution derivation tree and can be unfolded into a tree once the free parameter is instantiated. The expected properties of resolution and resolution derivations hold for resolution proof schema, more detail can be found in [8].

Definition 9 (Substitution Schema [8]). Let u_1, \dots, u_α be schematic variable symbols of type $\omega \rightarrow \iota$ and t_1, \dots, t_α be term schemata containing no other ω -variables than k . Then a substitution schema is an expression of the form $[u_1/\lambda k.t_1, \dots, u_\alpha/\lambda k.t_\alpha]$.

Semantically, the meaning of the substitution schema is for all $\gamma \in \mathbb{N}$ we have a substitution of the form $[u_1(\gamma)/\lambda k.t_1 \downarrow_\gamma, \dots, u_\alpha(\gamma)/\lambda k.t_\alpha \downarrow_\gamma]$. For the resolution proof schema the semantic meaning is as follows, Let $R(n) = (\varrho_1, \dots, \varrho_\alpha)$ be a resolution proof schema, θ be a clause substitution, ν an ω -variable substitution, ϑ be a substitution schema, and $\gamma \in \mathbb{N}$, then $R(\gamma) \downarrow$ denotes a resolution term which has a normal form of $\varrho_1(n, \overline{w}, \overline{u}, \overline{X})\theta\nu\vartheta[n/\gamma]$ w.r.t. R extended by rewrite rules for defined function and predicate symbols.

2.4 Herbrand Systems

From the resolution proof schema and the substitution schema we can extract a so-called *Herbrand system*. The idea is to generalize the mid sequent theorem of Gentzen to proof schemata [4,12]. This theorem states that a proof (cut-free or with quantifier-free cuts) of a prenex end-sequent can be transformed in a way that there is a midsequent separating quantifier inferences from propositional ones. The mid-sequent is propositionally valid (w.r.t. the axioms) and contains (in general several) instances of the matrices of the prenex formulas; it is also called a *Herbrand sequent*. The aim of this paper is to extract schematic Herbrand sequents from schematic cut-elimination via CERES. We restrict the sequents further to skolemized ones. In the schematization of these sequents we allow only the matrices of the formulas to contain schematic variables (the number of formulas in the sequents and the quantifier prefixes are fixed).

Definition 10 (skolemized prenex sequent schema). Let

$$S(n) = \Delta_n, \varphi_1(n), \dots, \varphi_k(n) \vdash \psi_1(n), \dots, \psi_l(n), \Pi_n, \text{ for } k, l \in \mathbb{N} \text{ where}$$

$$\varphi_i(n) = \forall x_1^i \dots \forall x_{\alpha_i}^i F_i(n, x_1^i, \dots, x_{\alpha_i}^i), \quad \psi_j(n) = \exists x_1^j \dots \exists y_{\beta_j}^j E_j(n, y_1^j, \dots, y_{\beta_j}^j),$$

for $\alpha_i, \beta_j \in \mathbb{N}$, F_i and E_j are quantifier-free schematic formulas and Δ_n, Π_n are multisets of quantifier-free formulas of fixed size; moreover, the only free variable in any of the formulas is $n : \omega$. Then $S(n)$ is called a *skolemized prenex sequent schema* (sps-schema).

Definition 11 (Herbrand System). Let $S(n)$ be a sps-schema as in Definition 10. Then a Herbrand system for $S(n)$ is a rewrite system \mathcal{R} (containing the

list constructors and unary function symbols w_i^x , for $x \in \{\varphi, \psi\}$, such that for each $\gamma \in \mathbb{N}$, the normal form of $w_i^x(\gamma)$ w.r.t \mathcal{R} is a list of list of terms $t_{i,x,\gamma}$ (of length $m(i, x)$) such that the sequent

$$\Delta_\gamma, \Phi_1(\gamma), \dots, \Phi_k(\gamma) \vdash \Psi_1(\gamma), \dots, \Psi_l(\gamma)$$

for

$$\begin{aligned} \Phi_j(\gamma) &= \bigwedge_{p=1}^{m(j,\varphi)} E_j(\gamma, t_{j,\varphi,\gamma}(p, 1), \dots, t_{j,\varphi,\gamma}(p, \alpha_j)) \quad (j = 1, \dots, k), \\ \Psi_j(\gamma) &= \bigvee_{p=1}^{m(j,\psi)} F_j(\gamma, t_{j,\psi,\gamma}(p, 1), \dots, t_{j,\psi,\gamma}(p, \beta_j)) \quad (j = 1, \dots, l), \end{aligned}$$

is **LKE**-provable.

Though our definition of a Herbrand system differs from the definition introduced in [8] (where only purely existential schemata are treated), it is only a minor syntactic generalization. All results proven in [8] carry over to this more general form above.

3 “Mathematical” Proof of the ECA Statement and Discussion of Formal Proof

For lack of space, we will not provide a formal proof of the ECA-schema in the **LKS**-calculus (see Appendix A), but rather a mathematical argument proving the statement, of which closely follows the intended formal proof. The ECA-schema can be stated as follows:

Theorem 1 (Eventually Constant Assertion). *Given a total monotonically decreasing function $f : \mathbb{N} \rightarrow \{0, \dots, n\}$, for $n \in \mathbb{N}$, then there exists an $x \in \mathbb{N}$ such that for all $y \in \mathbb{N}$, where $x \leq y$, it is the case that $f(x) = f(y)$.*

Proof. If the range only contains 0 then the theorem trivially holds. Let us assume it holds for a codomain with n elements and show it hold for a codomain with $n + 1$ elements. If for all positions x , $f(x) = n$ then the theorem holds, else if at some y , $f(y) \neq n$ then from that point on f cannot map to n because the function is monotonically decreasing, thus, f will only have n elements in its codomain and the theorem holds in this case by the induction hypothesis.

The cut consists of the case distinction made in the stepcase. When written in the **LKS**-calculus, it is as follows:

$$\exists x \forall y ((x \leq y) \rightarrow n + 1 = f(y)) \vee f(y) < n + 1$$

Notice that if we are to formalize the statement in the **LKS**-calculus the consequent has a $\exists \forall$ quantifier prefix:

$$\forall x (\bigvee_{i=0}^{n+1} i = f(x)), \forall x \forall y (x \leq y \rightarrow f(y) \leq f(x)) \vdash \exists x \forall y (x \leq y \rightarrow f(x) = f(y))$$

The CERES method (as well as the schematic CERES method) was designed for proofs without *strong quantification* in the end sequent. To get around this problem the proofs have to be *skolemized* [2]. We will not go into details of proof skolemization in this work, but to note, in the formal proof $g(\cdot)$, is the introduced skolem symbol.

4 Extraction of the Characteristic Term Schema

Each of the proof schema pairs of the formal proof (see Appendix A) have one cut configuration. In the case of ψ it is the empty configuration, and in the case of $\varphi(n)$ it is

$$\Omega(n) \equiv \exists x \forall y ((x \leq y) \rightarrow n + 1 = f(y)) \vee f(y) < n + 1.$$

This holds for the basecases as well as the stepcases. Thus, we have the following clause set terms:

$$CL_{ECA}(0) \equiv \Theta^{\psi, \emptyset}(0) \equiv cl^{\varphi, \Omega(0)}(0) \oplus (\{\vdash f(\alpha) < 0\} \otimes \{\vdash 0 = f(\alpha)\} \otimes \{0 \leq \beta \vdash\}) \quad (2a)$$

$$cl^{\varphi, \Omega(0)}(0) \equiv \Theta^{\varphi, \Omega(0)}(0) \equiv \{f(\alpha) < 0 \vdash\} \oplus \{f(g(\alpha)) < 0 \vdash\} \oplus \{\vdash \alpha \leq \alpha\} \oplus \{\vdash \alpha \leq g(\alpha)\} \oplus \{0 = f(\alpha), 0 = f(g(\alpha)) \vdash\} \quad (2b)$$

$$CL_{ECA}(n+1) \equiv \Theta^{\psi, \emptyset}(n+1) \equiv cl^{\varphi, \Omega(n+1)}(n+1) \oplus (\{\vdash f(\alpha) < n+1\} \otimes \{\vdash n+1 = f(\alpha)\} \otimes \{0 \leq \beta \vdash\}) \quad (2c)$$

$$cl^{\varphi, \Omega(n+1)}(n+1) \equiv \Theta^{\varphi, \Omega(n+1)}(n+1) \equiv cl^{\varphi, \Omega(n)}(n) \oplus \{n+1=f(\alpha), n+1=f(g(\alpha)) \vdash\} \oplus \{\vdash \alpha \leq \alpha\} \oplus \{\alpha \leq g(\alpha)\} \oplus \{n+1=f(\beta) \vdash n+1=f(\beta)\} \oplus \{\alpha \leq \beta \vdash \alpha \leq \beta\} \oplus \{f(\beta) < n+1 \vdash f(\beta) < n+1\} \oplus \{f(\alpha) < n+1, \alpha \leq \beta \vdash n=f(\beta), f(\beta) < n\} \quad (2d)$$

In the characteristic clause set schema $CL_{ECA}(n+1)$ presented in Eq.2 tautology and subsumption elimination have not been applied. Applying both types of elimination to $CL_{ECA}(n)$ and normalizing the clause set yields the following clause set $C(n)$:

$$\begin{aligned} C1(x, k) &\equiv \vdash x(k) \leq x(k) \\ C2(x, k) &\equiv \vdash x(k) \leq g(x(k)) \\ C3(x, i, k) &\equiv i = f(x(k)), i = f(g(x(k))) \vdash \\ C4(x, y, i, k) &\equiv y(k) \leq x(k), f(y(k)) < i + 1 \vdash \\ &\quad f(x(k)) < i, i = f(x(k)) \\ C4'(x, y, i, k) &\equiv y(k) \leq x(k+1), f(y(k)) < i + 1 \vdash \\ &\quad f(x(k+1)) < i, i = f(x(k+1)) \\ C5(x, k) &\equiv f(x(k)) < 0 \vdash \\ C6(x, k) &\equiv f(g(x(k))) < 0 \vdash \\ C7(x, k) &\equiv 0 \leq x(k) \vdash f(x(k)) < n, f(x(k)) = n \end{aligned}$$

We have introduced clause names, schematic variables, and an additional ω -variable which will be used in the refutation of Sec. 5.

5 Refutation of the Characteristic Clause set of the ECA-schema

We discovered the resolution refutation schema which we present here with the help of the SPASS theorem prover [13] in default mode, and with the flags for standard resolution and ordered resolution set. Various other modes of the theorem prover were tested, however, given that we needed to translate the resulting proof into the simple resolution language of [8], the chosen modes provided the easiest proofs for translation. After running the theorem prover on five instances of the clause set, we were able to extract an invariant for the resolution refutation schema. Essentially, the refutation differentiates between the symbols occurring in the codomain of f and not occurring. This is denoted using the function g . The excerpt from the SPASS output in Table 1 indicates the invariant. However, even though SPASS was able to provide a refutation for each instance, we could not use these refutations directly in the resolution refutation schema being that the SPASS output ignores the structural importance of the ω sort. Unlike the ordering problem of the NiA-schema [5,6], this choice made by SPASS was not necessary to the refutation of the ECA-schema and we were able to find a suitable refutation.

310[0:MRR:309.0,306.1]	$\vdash f(\alpha) < 3$
311[0:MRR:10.1,310.0]	$\alpha \leq \beta \vdash 2 = f(\beta) \quad f(\beta) < 2$
312[0:Res:2.0,311.0]	$\vdash 2 = f(\alpha) \quad f(\alpha) < 2$
314[0:Res:312.0,6.1]	$2 = f(\alpha) \vdash f(g(\beta)) < 2$
315[0:Res:314.1,11.1]	$2 = f(\alpha) \quad g(\alpha) \leq \beta \vdash 1 = f(\beta) \quad f(\beta) < 1$
316[0:Res:312.0,315.0]	$g(\alpha) \leq \beta \vdash f(\alpha) < 2 \quad 1 = f(\beta) \quad f(\beta) < 1$
317[0:Res:2.0,316.0]	$\vdash f(\alpha) < 2 \quad 1 = f(g(\alpha)) \quad f(g(\alpha)) < 1$
318[0:Res:3.0,316.0]	$\vdash f(\alpha) < 2 \quad 1 = f(g(g(\alpha))) \quad f(g(g(\alpha))) < 1$
321[0:Res:318.1,7.1]	$1 = f(g(\alpha)) \vdash f(\alpha) < 2 \quad f(g(g(\alpha))) < 1$
322[0:Res:321.2,14.1]	$1 = f(g(\alpha)) \quad g(g(\alpha)) \leq \beta \vdash f(\alpha) < 2 \quad 0 = f(\beta)$
325[0:Res:317.1,322.0]	$g(g(\alpha)) \leq \beta \vdash f(\alpha) < 2 \quad f(g(\alpha)) < 1 \quad f(\alpha) < 2 \quad 0 = f(\beta)$
327[0:Obv:325.1]	$g(g(\alpha)) \leq \beta \vdash f(g(\alpha)) < 1 \quad f(\alpha) < 2 \quad 0 = f(\beta)$
328[0:Res:2.0,327.0]	$\vdash f(g(\alpha)) < 1 \quad f(\alpha) < 2 \quad 0 = f(g(g(\alpha)))$
329[0:Res:3.0,327.0]	$\vdash f(g(\alpha)) < 1 \quad f(\alpha) < 2 \quad 0 = f(g(g(g(\alpha))))$
335[0:Res:329.2,8.1]	$0 = f(g(g(\alpha))) \vdash f(g(\alpha)) < 1 \quad f(\alpha) < 2$
336[0:MRR:335.0,328.2]	$\vdash f(g(\alpha)) < 1 \quad f(\alpha) < 2$
337[0:Res:336.0,14.1]	$g(\alpha) \leq \beta \vdash f(\alpha) < 2 \quad 0 = f(\beta)$
338[0:Res:2.0,337.0]	$\vdash f(\alpha) < 2 \quad 0 = f(g(\alpha))$
339[0:Res:3.0,337.0]	$\vdash f(\alpha) < 2 \quad 0 = f(g(g(\alpha)))$
344[0:Res:339.1,8.1]	$0 = f(g(\alpha)) \vdash f(\alpha) < 2$
345[0:MRR:344.0,338.1]	$\vdash f(\alpha) < 2$

Table 1. Excerpt from SPASS output for the clause set instance $C(5)$ indicating the invariant.

Our resolution refutation schema of the ECA-schema is $\mathcal{R} = (\varrho_1, \dots, \varrho_{10})$, where we use one clause variable Y , two schematic variables, and one ω -variable. Our substitution schema is as follows:

$$\vartheta = \{x(k) \leftarrow \lambda k.(h(k)), y(k) \leftarrow \lambda k.(h(k))\}$$

where $h(\cdot)$ is defined as $h(0) \rightarrow 0$, $h(s(k)) \rightarrow g(h(k))$. The components are as follows:

$$\varrho_1(n+1, k, x, y, Y) \Rightarrow r(\varrho_2(n+1, k, x, y, Y); \varrho_5(n, k, x, y, Y \circ (f(x(k)) < n+1 \vdash)); f(x(k)) < n+1)$$

$$\varrho_1(0, k, x, y, Y) \Rightarrow r(\varrho_2(0, k, x, y, Y); C5(x, k); f(x(k)) < 0)$$

$$\varrho_2(n+1, k, x, y, Y) \Rightarrow r(\varrho_3(n+1, k, x, y, Y); r(C1(x, k); C7(x, k); x(k) \leq x(k)); n+1 = f(x(k)))$$

$$\varrho_2(0, k, x, y, Y) \Rightarrow r(\varrho_3(0, k, x, y, Y); r(C1(x, k); C7(x, k); x(k) \leq x(k)); n+1 = f(x(k)))$$

$$\varrho_3(n+1, k, x, y, Y) \Rightarrow r(\varrho_4(n+1, k, x, y, Y); C3(x, n+1, k); n+1 = f(g(x(k))))$$

$$\varrho_3(0, k, x, y, Y) \Rightarrow r(\varrho_4(0, k, x, y, Y); C3(x, 0, k); 0 = f(g(x(k))))$$

$$\varrho_4(n+1, k, x, y, Y) \Rightarrow r(\varrho_5(n, k+1, x, y, Y \circ f(x(k+1)) < n+1 \vdash); r(C2(x, k); C7(x, k+1); f(x(k+1)) < n+1))$$

$$\varrho_4(0, k, x, y, Y) \Rightarrow r(C6(x, k); r(C2(x, k); C7(x, k+1); f(g(x(k))) < 0))$$

$$\varrho_5(n+1, k, x, y, Y) \Rightarrow r(\varrho_6(n+1, k, x, y, Y); \varrho_5(n, k, x, y, Y \circ (f(x(k)) < n+1 \vdash)); f(x(k)) < n+1)$$

$$\varrho_5(0, k, x, y, Y) \Rightarrow r(\varrho_6(0, k, x, y, Y); C5(x, k); f(x(k)) < 0)$$

$$\varrho_6(n+1, k, x, y, Y) \Rightarrow r(\varrho_7(n+1, k, x, y, Y); \varrho_8(n+1, k, x, y, Y); n+1 = f(x(k)))$$

$$\varrho_6(0, k, x, y, Y) \Rightarrow r(\varrho_7(0, k, x, y, Y); \varrho_8(0, k, x, y, Y); 0 = f(x(k)))$$

$$\begin{aligned}
\varrho_7(n+1, k, x, y, Y) &\Rightarrow r(\varrho_9(n+1, k, x, y, Y); C3(x, n+1, k); \\
&\quad n+1 = f(g(x(k)))) \\
\varrho_7(0, k, x, y, Y) &\Rightarrow r(\varrho_9(0, k, x, y, Y); C3(x, 0, k); 0 = f(g(x(k)))) \\
\varrho_8(n+1, k, x, Y) &\Rightarrow r(C1(x, k); Y \circ C4(x, y, n, k); x(k) \leq x(k)) \\
\varrho_8(0, k, x, y, Y) &\Rightarrow r(C1(x, k); Y \circ C4(x, y, 0, k); x(k) \leq x(k)) \\
\varrho_9(n+1, k, x, y, Y) &\Rightarrow r(\varrho_5(n, k+1, x, y, Y' \circ f(g(x(k))) < n+1 \vdash); \\
&\quad \varrho_{10}(n+1, x, y, Y); f(g(x(k))) < n+1) \\
\varrho_9(0, k, x, y, Y) &\Rightarrow r(C6(x, k); \varrho_{10}(0, k, x, y, Y); f(g(x(k))) < 0) \\
\varrho_{10}(n+1, k, x, y, Y) &\Rightarrow r(C2(x, k); Y \circ C4'(x, y, n, k); x(k) \leq g(x(k))) \\
\varrho_{10}(0, k, x, y, Y) &\Rightarrow r(C2(x, k); Y \circ C4'(x, y, 0, k); x(k) \leq g(x(k)))
\end{aligned}$$

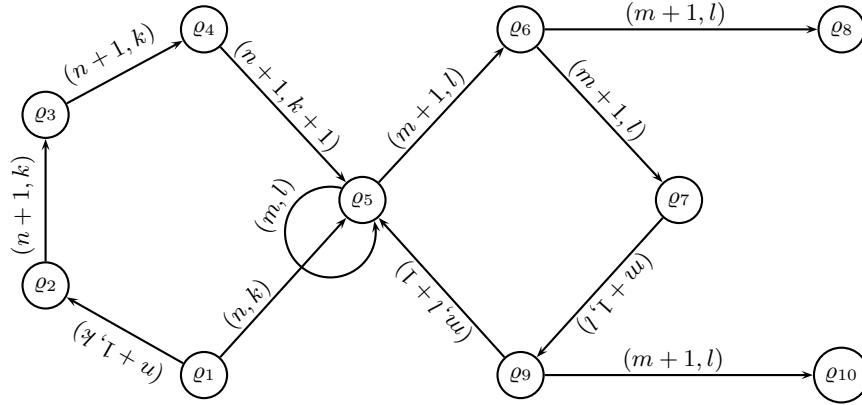


Fig. 1. A graph representation of the resolution refutation. The variable n is the free parameter, k is the ω -variable used in the refutation and the variables m and l are dependent on the position in the computation.

One can find a graphical representation of the refutation in Fig. 1. The clause substitution is $\theta = \{Y \leftarrow \vdash\}$, the ω -variable substitution is $\nu = \{k \leftarrow \bar{\mu}\}$ for any $\bar{\mu} \in \mathbb{N}$. The normal form of the refutation for $\gamma \in \mathbb{N}$ is

$$\varrho_1(n, k, x, y, Y)\theta\nu\vartheta[n \leftarrow \gamma] = \varrho_1(\gamma, \bar{\mu}, \lambda_k.(i_s(k)), \lambda_k.(h(k)), \vdash),$$

where $i_s(0) = 0$, $i_s(s(k)) = s(i_s(k))$. Substitution of the empty clause into Y suffices for every instance, i.e. $\{Y \leftarrow \vdash\}$. This property makes extraction of the Herbrand system much easier.

6 The Herbrand System for the ECA-schema

Now we move on to the construction of a Herbrand system for the sequent

$$S(n) \equiv (\forall x \bigvee_{i=0}^n i = f(x), \forall y (0 \leq y \rightarrow f(y) \leq f(0))) \vdash \\ \exists x (x \leq g(x) \rightarrow f(x) = f(g(x)))$$

based on our proof analysis. The sequent $S(n)$ is an sps-schema of the form $\varphi_1(n), \varphi_2(n) \vdash \psi_1(n)$. Note that we dropped one of the quantifiers from the antecedent being that it is obvious from the proof itself what the substitution would be, see Appendix A. Each formula in $S(n)$ is derived along with a set of clauses in the proof schemata $\Psi = \langle (\psi(n+1), \psi(0)), (\varphi(n+1), \varphi(0)) \rangle$. By observing the construction of the formulae in Appendix A.2 and Appendix A.4, one can see that $\varphi_1(n)$, $\varphi_2(n)$, and $C7(x, k)$ as constructed together, while $\psi_1(n)$, $C2(x, k)$, and $C3(x, i, k)$ are constructed together. We will only consider the case when the ω -variable substitution is $\nu = \{k \rightarrow 0\}$ to simplify the derivation.

Notice that $C7(x, k)$ is used at the top of the refutation and only twice. Once as $C7(x, 0)$ and once as $C7(x, 1)$. On the other hand, $C2(x, k)$ is used in ϱ_{10} and $C3(x, i, k)$ is use in ϱ_7 . For every pair (i, l) in the ranges $0 \leq i \leq n+1, 0 \leq l < n+1$, the clauses $C2(x, l)$ and $C3(x, i, l)$, and $C2(x, l+1)$ and $C3(x, i, l+1)$ are used in the refutation. This implies, by the substitution schema that $\psi_1(n)$ will have its quantifier replaced by the term derived from $h(i)$, for all $i \in [0, n]$, in the Herbrand system. This information can be used to construct the required rewrite system:

$$\mathcal{R} = \begin{cases} w_1^\varphi(k+1) \Rightarrow [[0]; [g(0)]] \\ w_1^\varphi(0) \Rightarrow [[0]; [g(0)]] \\ w_2^\varphi(k+1) \Rightarrow [[0]; [g(0)]] \\ w_2^\varphi(0) \Rightarrow [[0]; [g(0)]] \\ w_1^\psi(k+1) \Rightarrow [[h(k+1)]; w_1^\psi(k)] \\ w_1^\psi(0) \Rightarrow [0] \end{cases}$$

To finish our construction of the Herbrand system using Def. 11 We need to put all of the parts together as a single sequent as follows

$$\bigvee_{i=0}^n i = f(0), \bigvee_{i=0}^n i = f(g(0)), (0 \leq 0 \rightarrow f(0) \leq f(0)), \\ (0 \leq g(0) \rightarrow f(g(0)) \leq f(0)) \vdash \bigvee_{i=0}^n (h(i) \leq g(h(i)) \rightarrow f(h(i)) = f(g(h(i)))) .$$

At first this does not seem to be **LKE** provable, However, one has to remember that for the construction of our cut formula we made an assumption that f is monotonically decreasing and has a codomain consisting of elements in the

interval $[0, n]$. These assumptions are represented by the following axiom found in Appendix A:

$$AX \equiv f(\alpha) < n + 1, \alpha \leq \beta \vdash n = f(\beta), f(\beta) < n$$

It is not used in the construction of the end sequent but is used for the construction of the cut formulae. We just need to find a set of axioms which correspond to these semantic assumptions, the following set suffices:

$$\begin{aligned} A1(i) : & \bigvee_{i=0}^{j-1} i = f(\alpha), j = f(g(\alpha)), f(g(\alpha)) < f(\alpha) \vdash \\ A2(i) : & i = f(\alpha), \bigvee_{j=0}^{i-1} j = f(g(\alpha)), \alpha \leq g(\alpha) \vdash \\ A3(i) : & i = f(\alpha), i = f(g(\alpha)) \vdash f(\alpha) = f(g(\alpha)) \\ A4(i) : & f(g(\alpha)) = f(\alpha) \vdash f(\alpha) = f(g(\alpha)) \\ A5(i) : & \vdash \alpha \leq \alpha \\ A6(i) : & f(\alpha) < f(\alpha) \vdash \end{aligned}$$

The first pair of axioms enforce the required properties of f and g , the next pair provide the needed properties of equality, and the last pair provide the needed properties of linear orderings. Interesting enough, using these axioms, we are able to prove the derived Herbrand sequent using only a single nesting of g , thus making the majority of the consequent redundant. This is a result of our usage of the clause $C7(x, k)$. Thus, it turns out that a minimal Herbrand sequent is the following:

$$\begin{aligned} & \bigvee_{i=0}^n i = f(0), \bigvee_{i=0}^n i = f(g(0)), (0 \leq g(0) \rightarrow f(g(0)) \leq f(0)), \\ & (0 \leq 0 \rightarrow f(0) \leq f(0)) \vdash 0 \leq g^1(0) \rightarrow f(0) = f(g^1(0)). \end{aligned}$$

The Herbrand sequent can be derived for deeper nestings of g by changing the ω -variable substitution used.

7 Conclusion

Weakening the NiA-schema of [5] by reducing the complexity of the cuts allowed for extraction of the Herbrand system using the concepts of [8]. As a case study of the schematic CERES method, to the best of our knowledge this is the first one. From the analysis of the ECA-schema there are two issues which seem to influence the applicability of the schematic CERES method. The first issue, as we pointed out earlier, is the ordering of the terms in the ω sort. However, a second issue arising in this work is the complexity of the terms, specifically what is the highest arity function symbol allowed. In the case of the NiA-schema, terms were constructed from both an arity two and an arity one function symbol, but in the case of the ECA-schema only arity one function symbols were used. When only arity one function symbols are used nesting of the function symbols does not require the addition of *extra variables* in a given term, of which were used

in the NiA-schema [5,6]. This seems to allow for the creation of more complex orderings of the ω sort. We conjecture a sufficient condition that proof schema containing only arity one function symbols can be analysed using the schematic CERES method. Also, an open problem we plan to address in future work is a generalization of the resolution refutation calculus of [8] which can handle more complex ordering structures[6]. It seems necessary to handle more complex ordering structure if one wants to formalize and analyse more complex mathematical arguments such as Fürstenberg’s proof of the infinitude of primes.

References

1. Matthias Baaz, Stefan Hetzl, Alexander Leitsch, Clemens Richter, and Hendrik Spohr. Ceres: An analysis of Fürstenberg’s proof of the infinity of primes. *Theoretical Computer Science*, 403(2-3):160–175, August 2008.
2. Matthias Baaz and Alexander Leitsch. On skolemization and proof complexity. *Fundamenta Informaticae*, 20(4):353–379, December 1994.
3. Matthias Baaz and Alexander Leitsch. Cut-elimination and redundancy-elimination by resolution. *Journal of Symbolic Computation*, 29:149–176, 2000.
4. Matthias Baaz and Alexander Leitsch. *Methods of Cut-Elimination*. Springer Publishing Company, Incorporated, 2013.
5. David Cerna and Alexander Leitsch. Analysis of clause set schema aided by automated theorem proving: A case study, 2015. arXiv:1503.08551v1 [cs.LO].
6. David M. Cerna. *Advances in schematic cut elimination*. PhD thesis, Technical University of Vienna, 2015. <http://media.obvsg.at/p-AC12246421-2001>.
7. cvetan Dunchev. *Automation of cut-elimination in proof schemata*. PhD thesis, Technical University of Vienna, 2012.
8. Cvetan Dunchev, Alexander Leitsch, Mikheil Rukhaia, and Daniel Weller. Cut-elimination and proof schemata. *Journal of Language, Logic, and Computation*, 2014.
9. Gerhard Gentzen. Untersuchungen über das logische Schließen I. *Mathematische Zeitschrift*, 39(1):176–210, December 1935.
10. Jean-Yves Girard. *Proof theory and logical complexity*, volume I of *Studies in proof theory*. Bibliopolis, 1987.
11. Raymond McDowell and Dale Miller. Cut-elimination for a logic with definitions and induction. *Theoretical Computer Science*, 232:2000, 1997.
12. Gaisi Takeuti. *Proof Theory*, volume 81 of *Studies in logic and the foundations of mathematics*. American Elsevier Pub., 1975.
13. Christoph Weidenbach, Dilyana Dimova, Arnaud Fietzke, Rohit Kumar, Martin Suda, and Patrick Wischnewski. Spass version 3.5. In *Proceedings of the 22Nd International Conference on Automated Deduction, CADE-22*, pages 140–145, Berlin, Heidelberg, 2009. Springer-Verlag.

A ECA Formalized in the LKS-calculus

In our **LKS**-calculus, cut ancestors have a * and cut-configuration ancestors have a **. The proof has already been skolemized. We will make the following abbreviations to simplify the formal proof:

$$ESC \equiv \exists x(x \leq g(x) \rightarrow f(x) = f(g(x))),$$

$$MD \equiv \forall x \forall y (x \leq y \rightarrow f(y) \leq f(x)),$$

$$FD(n) \equiv \forall x (\bigvee_{i=0}^n i = f(x)) ,$$

$$CUT \equiv \exists x \forall y ((x \leq y) \rightarrow n+1 = f(y) \vee f(y) < n+1),$$

$$AX \equiv f(\alpha) < n+1^*, \alpha \leq \beta^* \vdash n = f(\beta)^*, f(\beta) < n^*.$$

Also, We will remove every inference rule which does not influence the characteristic clause set of the ECA-schema.

$$\begin{array}{c}
 \vdots \\
 \vdots \\
 \hline \bigvee_{i=0}^n i = f(\beta) \vdash \\
 f(\beta) < n+1^* \\
 \vdots \\
 \vdots \\
 \hline
 \begin{array}{ccc}
 \vdots & n+1 = f(\beta) \vdash & \\
 \vdots & n+1 = f(\beta)^* & \\
 \vdots & & \\
 \hline
 \vdots & & 0 \leq \beta^* \vdash \\
 \vdots & & 0 \leq \beta \\
 \hline
 \vdots & & \rightarrow : l
 \end{array}
 \end{array}
 \quad \vee : l$$

$$\begin{array}{ccc}
 \vdots & & \varphi(n+1) \\
 \hline
 FD(n+1), MD \vdash CUT(n+1)^* & & CUT(n+1)^* \vdash ESC \\
 \hline
 FD(n+1), MD \vdash ESC & & cut
 \end{array}$$

Fig. 2. Proof symbol $\psi(n+1)$

$$\begin{array}{c}
 \hline 0 = f(\alpha) \vdash 0 = f(\alpha)^* \\
 \vdots \\
 \vdots \\
 \hline
 \vdots & 0 \leq \alpha^* \vdash 0 \leq \alpha \\
 \vdots & \\
 \hline
 \vdots & \rightarrow : l
 \end{array}$$

$$\begin{array}{ccc}
 \vdots & & \varphi(0) \\
 \hline
 FD(0), MD \vdash CUT(0)^* & & CUT(0)^* \vdash ESC \\
 \hline
 FD(0), MD \vdash ESC & & cut
 \end{array}$$

Fig. 3. Proof symbol $\psi(0)$

$$\begin{array}{c}
\frac{n+1 = f(\beta)^{**} \vdash \quad \alpha \leq \beta^* \vdash}{n+1 = f(\beta)^* \quad \alpha \leq \beta^{**}} \rightarrow: l \\
\vdots \\
\vdots \\
\frac{f(\beta) < n+1^{**} \vdash \quad f(\beta) < n+1^* \vdash}{\vdots} \vee: l \\
\vdots \\
\vdots \\
\frac{AX}{(1)} cut \\
\\
\frac{n+1 = f(\alpha)^*, \quad n+1 = f(g(\alpha))^* \vdash \quad \vdash \alpha \leq \alpha^*}{f(\alpha) = f(g(\alpha))} \rightarrow: l \\
\vdots \\
\vdots \\
\frac{\alpha \leq g(\alpha) \vdash \quad \alpha \leq g(\alpha)^*}{\vdots} \rightarrow: l \\
(1) \quad \frac{CUT(n+1)^{**} \vdash CUT(n)^*, ESC}{\vdots} cut \\
\vdots \\
\frac{CUT(n+1)^{**} \vdash ESC, ESC \quad \varphi(n) \quad \dots \quad CUT(n)^* \vdash ESC}{CUT(n+1)^{**} \vdash ESC} cut \\
\frac{CUT(n+1)^{**} \vdash ESC, ESC}{CUT(n+1)^{**} \vdash ESC} c: l
\end{array}$$

Fig. 4. Proof symbol $\varphi(n+1)$

$$\begin{array}{c}
\frac{0 = f(\alpha)^{**}, \quad 0 = f(g(\alpha))^{**} \vdash \quad \alpha \leq g(\alpha) \vdash \quad \alpha \leq g(\alpha)^{**}}{f(\alpha) = f(g(\alpha))} \rightarrow: l \\
\vdots \\
\vdots \\
\frac{\vdash \alpha \leq \alpha^{**}}{\vdots} \rightarrow: l \\
\vdots \\
\vdots \\
\frac{f(g(\alpha)) < 0^{**} \vdash}{\vdots} \vee: l \\
\vdots \\
\vdots \\
\frac{f(\alpha) < 0^{**} \vdash}{\vdots} \vee: l \\
\vdots \\
\vdots \\
\frac{CUT(0)^{**} \vdash ESC}{\vdots}
\end{array}$$

Fig. 5. Proof symbol $\varphi(0)$

B Example Resolution Refutation

$$\begin{array}{c}
\begin{array}{c}
C6(x, 0, 2) \quad \frac{\frac{C2(x, 0, 2) \quad C4'(x, y, 0, 2)}{f(g(g(0))) < 1 \vdash 0 = f(g(g(g(0))))}, f(g(g(g(0)))) < 0}{f(g(g(0))) < 1 \vdash 0 = f(g(g(g(0))))} \\
\hline
f(g(g(0))) < 1, 0 = f(g(g(0))) \vdash (6) \quad C3(x, 0, 2)
\end{array} \\
\\
\begin{array}{c}
\frac{\frac{f(g(g(0))) < 1, \quad 0 = f(g(g(0))) \vdash (6) \quad \frac{C1(x, 0, 2) \quad C4(x, 0, 2)}{f(g(g(0))) < 1 \vdash 0 = f(g(g(0))), f(g(g(0))) < 0}}{f(g(g(0))) < 1 \vdash f(g(g(0))) < 0} \\
\hline
f(g(g(0))) < 1 \vdash (D) \quad C5(x, 0, 2)
\end{array}
\end{array}$$

Fig. 6. Resolution refutation for instance $n = 2$ and $k = 0$ (Part B).

$$\begin{array}{c}
\frac{C6(x, 0, 1) \quad \frac{C2(x, 0, 1) \quad C4'(x, y, 0, 1)}{f(g(0)) < 1 \vdash 0 = f(g(g(0))), f(g(g(0))) < 0}}{f(g(0)) < 1 \vdash 0 = f(g(g(0)))} \quad C3(x, 0, 1) \\
\hline
f(g(0)) < 1, 0 = f(g(0)) \vdash (5)
\end{array}$$

$$\begin{array}{c}
\frac{f(g(0)) < 1, 0 = f(g(0)) \vdash (5) \quad \frac{C1(x, 0, 1) \quad C4(x, y, 0, 1)}{f(g(0)) < 1 \vdash 0 = f(g(0)), f(g(0)) < 0}}{f(g(0)) < 1 \vdash f(g(0)) < 0} \quad C5(x, 0, 1) \\
\hline
f(g(0)) < 1 \vdash (C)
\end{array}$$

$$\begin{array}{c}
\frac{C6(x, 0, 0) \quad \frac{C2(x, 0, 0) \quad C4'(x, y, 0, 0)}{f(0) < 1 \vdash 0 = f(g(0)), f(g(0)) < 0}}{f(0) < 1 \vdash 0 = f(g(0))} \quad C3(x, 0, 0) \\
\hline
f(x(1, 0)) < 1, 0 = f(x(0, 0)) \vdash (4)
\end{array}$$

$$\begin{array}{c}
\frac{f(0) < 1, 0 = f(0) \vdash (4) \quad \frac{C1(x, 0, 0) \quad C4(x, y, 0, 0)}{f(0) < 1 \vdash 0 = f(0), f(0) < 0}}{f(0) < 1 \vdash f(0) < 0} \quad C5(x, 0, 0) \\
\hline
f(0) < 1 \vdash (E)
\end{array}$$

$$\begin{array}{c}
\frac{f(g(g(0))) < 1 \vdash (D) \quad \frac{C2(x, 1, 1) \quad C4'(x, y, 1, 1)}{f(g(0)) < 2 \vdash 1 = f(g(g(0))), f(g(g(0))) < 1}}{f(g(0)) < 2 \vdash 1 = f(g(g(0)))} \quad C3(x, 1, 1) \\
\hline
f(g(0)) < 2, 1 = f(g(0)) \vdash (3)
\end{array}$$

$$\begin{array}{c}
\frac{f(g(0)) < 2, 1 = f(g(0)) \vdash (3) \quad \frac{C1(x, 1, 1) \quad C4(x, y, 1, 1)}{f(g(0)) < 2 \vdash 1 = f(g(0)), f(g(0)) < 1}}{f(g(0)) < 2 \vdash f(g(0)) < 1} \quad f(g(0)) < 1 \vdash (C) \\
\hline
f(g(0)) < 2 \vdash (B)
\end{array}$$

$$\begin{array}{c}
\frac{f(g(0)) < 1 \vdash (C) \quad \frac{C2(x, 1, 0) \quad C4'(x, y, 1, 0)}{f(0) < 2 \vdash 1 = f(g(0)), f(g(0)) < 1}}{f(0) < 2 \vdash 1 = f(g(0))} \quad C3(x, 1, 0) \vdash \\
\hline
f(0) < 2, 1 = f(0) \vdash (2)
\end{array}$$

$$\begin{array}{c}
\frac{f(0) < 2, 1 = f(0) \vdash (2) \quad \frac{C1(x, 1, 0) \quad C4(x, y, 1, 0)}{f(0) < 2 \vdash 1 = f(0), f(0) < 1}}{f(0) < 2 \vdash f(0) < 1} \quad f(0) < 1 \vdash (E) \\
\hline
f(0) < 2 \vdash (A)
\end{array}$$

$$\begin{array}{c}
\frac{f(g(0)) < 2 \vdash (B) \quad \frac{C2(x, 2, 0) \quad C7(x, 2, 1)}{\vdash 2 = f(g(0)), f(g(0)) < 2}}{\vdash 2 = f(g(0))} \quad C3(x, 2, 0) \\
\hline
2 = f(0) \vdash (1)
\end{array}$$

$$\begin{array}{c}
\frac{2 = f(0) \vdash (1) \quad \frac{\vdash C1(x, 2, 0) \quad C7(x, 2, 0)}{\vdash 2 = f(0), f(0) < 2}}{\vdash f(0) < 2} \quad f(0) < 2 \vdash (A) \\
\hline
\vdash
\end{array}$$

Fig. 7. Resolution refutation for instance $n = 2$ and $k = 0$ (Part A).